Mehul Singh

+1 (437) 669 0427 / mehulsingh11@gmail.com / mehulsingh.in / mehul-singh-0x00 / @xmehulx

Skills: Automation, CLI, CRM, CTI, Debugging, DLP, DR, EDR, Firewall, GRC, IAM, IR, ITGC, ITSM, Linux/Unix, Networking, RCA, Reporting, Risk Advisory, Scripting, SIEM, Threat Modeling, Threat Hunting, VAPT, Windows

Tools: Azure AD, BloodHound, Burp Suite, Cymulate, MetricStream, Metasploit, Nessus, Nikto, Palo Alto, ProcessUnity, Proxychains, Recorded Future, Responder, SentinelOne, ServiceNow, Splunk, Wireshark

Certifications

OSCP, OffSec (On the way!); Security+, CompTIA; Certified in Cybersecurity, ISC2; NIST RMF, LinkedIn; Cybersecurity Professional, Google; Certified Network Security Specialist, ICSI; Network Security Associate, Fortinet; Cybersecurity (Basics+Essential), Cisco; Problem Solving (Basic+Intermediate), HackerRank;

Statement of Summary

Cybersecurity professional with **3+ years** in **threat hunting**, **incident response**, and **detection engineering**, including developing and **tuning threat detection** content, and 2+ years **advising senior leadership** in global enterprises on **risk assessments** and regulatory compliance. Experienced in threat intelligence analysis, attack techniques, and **adversary simulation**, with hands-on knowledge of **SIEM**, **IDS/IPS**, and **EDR** platforms. Skilled in translating complex **threats into actionable decisions** across cross-functional teams. Otherwise an **engineer** at heart with numerous personal projects like home VPN, NAS server, and ad/tracker-blocker on different platforms.

Education

Masters in Information Technology Security Sep 2023 - May 2025
Business&IT, Ontario Tech University, Oshawa, ON **GPA: 4.10/4.30**

Bachelors in Computer Science and Engineering 2017-2021
Engineering&Technology, Amity University, Noida, India **GPA: 8.84**

Work Experience

Security Analyst Co-op **Jan – Apr 2025**
Intact Financial Corporation

Technical Skills: CTI, GRC, Cymulate, Anomaly Detection, Incident Response, Vendor Assessment
Interpersonal Skills: Communication, Reporting, Coordination, Collaboration, Stakeholder Management, Analysis

- Provided new workflow for enhanced classification metrics and assessment intake process, reducing assessment turnarounds by 20%.
- Developed queries based on Cyber Threat Intelligence inputs which decreased false positives by 15%.
- Streamlined risk registers, derogations, and third-party risk assessment-related activities which increased visibility of risks and reduced operation time by 20%.
- Executed periodical review procedures for IT security procedures by producing relevant reports and by following up with accountable stakeholders following OSFI, PIPEDA and PHIPA.
- Took extended assignments under red-team and worked with the WAF team during investigations and increased automated detection and response by 25%.
- Update IoCs and playbooks based on observed trends post data gathering, analysis and process reviews.

Graduate Teaching Assistant **Sep – Dec 2024**
Advanced Communication Networks, Ontario Tech University
Advanced Network Security, Ontario Tech University

Technical Skills: OpenStack, OS Security, Network Architecture, Security & Virtualization, QoS, Firewall, VPN, WAF
Interpersonal Skills: Communication, Mentoring, Time Management, Empathy, Analytical Thinking, Leadership

- Offer individual and group support to students, helping with assignments, projects, and coursework.

- Conducted technical lab sessions and managed individual and group-based tasks.
- Work with lead instructors to design and deliver engaging lesson plans aligned with institutional goals.
- Attended 10+ industry conferences and events to collaborate and network with experts, leading to better understanding of my teaching strategy and a 96% satisfaction level from students in the end-term survey.
- Assessed, graded, provided feedback, and monitored student progress continuously.

Risk and Control Analyst **2021-2023**

Shell PLC, India

Technical Skills: Splunk, SonarQube, Risk Assessment, PKI, Incident Response, GRC, Firewall, Client Support
Interpersonal Skills: Communication, Reporting, Coordination, Collaboration, Problem Solving, Analysis

- Triaged 560+ security incidents and performed detailed rule and policy reviews as a Firewall subject matter expert, ensuring alignment with security protocols and risk tolerance thresholds.
- Performed vulnerability assessments of numerous applications using manual and automated tools, successfully identifying threats, and IoAs and advising mitigations, resulting in almost 20% lower KRIs.
- Co-led two firewall audits to successful outcomes, despite being an undergraduate hire.
- Adhered to standards like NIST SP 800-53, ISO 27001, and GDPR, ensuring that identified vulnerabilities and risks were documented and addressed in-line with compliance requirements.
- Collaborated and liaised with various cross-functional teams and MSSPs, and engaged with broader community to drive awareness regarding information security issues.
- Utilized ServiceNow and MetricStream to manage and track threat and vulnerability issues, closing them with thorough Findings' Management and updating Risk Registers on the enterprise tool.

Network Administrator Intern **May – Aug 2019**

ONGC Ltd., India

Technical Skills: Threat Detection, Network Analysis and Troubleshooting, Security Reviews, Cloud SaaS
Interpersonal Skills: Judgment, Requirement Gathering, independent work, Reporting

- Tasked with setting-up network devices including Juniper MX, EX and SRX series into the core network.
- Gained teamwork experience while helping the core team of around 9 people in their daily activities.
- Monitored network traffic, identifying and resolving over 400 anomalies; improved system reliability by addressing false positives that reduced congestion and packet drops across the core network.

Projects & Activities (complete on GitHub)

Red-Team Roadmap Notes/Journey **2022 - Active**

Technology: Toolkits, Unix, Windows, Kali, C, Bash, Python, Powershell
Skills: Scripting, Pen-testing, TTPs, Threat Analysis, Logical Reasoning, Problem-Solving, Troubleshooting

- HackTheBox "Pro Hacker" with 70+ machines exploited.
- 50+ CTFs attended, consistently being in the top 30% (6th position in TACOPS 2025).

Log4Shell Sandbox **2024**

Technology: Nmap, Metasploit, Nessus, Java, LDAP, Linux, Networking, Hypervisor
Skills: OWASP, Code Review, DevOps, Exploit Development, Network Monitoring, Scripting

Hybrid Load Balancer **2023**

Technology used: Terminal, Mininet, Wireshark, Networking, Python, Bash
Skills: Security Controls, Firewall configuration, SIEM, Performance Monitoring, Testing, Leadership

Network Packet Sniffer **2021**

Technology used: Python, Terminal, Networking, GitHub
Skills: Wireless Scanning, Requirement Gathering, Risk Reporting, Problem Solving